"GLOBAL SCENARIO OF CYBER CRIME AND SECURITY PROVISIONS IN COMPARISON WITH LEGAL RESPONSES IN INDIA"

Ph.D. synopsis submitted

To

Swami Ramanand Teerth Marathwada University,

Nanded-431606

Submitted by

Mrs Nivedita Babulal Jadhav

(BSL, LLM, DCL)

Assistant Professor

Under the Guidance of

Dr.Bande .Trimbak. M

Assistant Professor
Shivaji Law college, Kandhar
Dist. Nanded

GLOBAL SCENARIO OF CYBER CRIME AND SECURITY PROVISIONS IN COMPARISON WITH LEGAL RESPONSES IN INDIA

INTRODUCTION

'Nothing is permanent in the world, except one thing and that is the change.' Taking into consideration this line if we look into the area of crime, we see that the nature and the mode of crimes are also changing with the emergence and development of the science and technology.

Crime and criminality have been associated with man since time in memorial. Crime remains difficult to describe and even make strenuous effort to hide itself in the face of development. Success in any field of human activity leads to crime that needs mechanisms to control it.

The word "cyber" is referring to the science of "cybernetics" it derives from the Greek verb "kubernao" which means to steer which is the root of our present word to govern the idea behind it is navigation through a space of electronic data. Today the term of cyber is generally used when we speak about the computer. Now a day's computer is used in each sector like communication, railways, banking air travel, education, medical, agricultures, industry, judiciary, advocacy, and engineering.

Human intelligence brought in technological and information revolutions in the society. The progress of civilizations, as evidenced by the ever- changing information technology ,easily accessible by use of computers was no doubt put to use for improvement in standard of living of human beings. Information technology has become a valuable source for development of commerce, communication, entertainment and companionship. It has affected human life in every respect around the world.

Cyber crime involves criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief. The abuse of computers has also given birth to a gamut of new age crimes such as hacking, web defacement, cyber stalking, web jacking, etc.

Legal provisions should provide assurance to users, empowerment to law enforcement agencies and deterrence to criminals. The law is as stringent as its enforcement. Crime is no

longer limited to space, time or a group of people. Cyber space creates civil liability and criminal liability.

Whenever one touches a computer, computer system or computer network or any other computer resource one shall be the ambit of the Information Technology. I.T. has its effect as well as its defect, also on one hand it facilitates of the human life and on other hand it harm to it. The use of technology is growing day by day throughout the world. Crime as its defect is one of the major problem regarding the technology.

The legal definition of crime means 'any act or omission forbidden by law'. In modern world people started to commit crime with the help of available technology. Due to the lack of regulation in this area traditional law was applied but this is not enough to control all types of cyber crime. The nature of the cyber crime is the transboundry related to virtual space hence the existing laws were not sufficient to curb it.

The meaning of the cyber crime given in various dictionaries is very easy to understand what cyber crime means is, "cyber crime means crime committed over the internet." and also in another dictionary, "cyber crime means a crime involving the use of a computer such as sabotaging or stealing electronically stored data."

The last decade has been proven most significant in human history. In this decade the Internet and the worldwide web have flourished their own. Internet has set up new standard for the entire mankind. It all began in 1969 when America's Department of Defence commissioned construct a Super Network called ARPANET. Internet has grown in a very rapid, arbitrary and unplanned manner. Because of this unplanned nature of Internet is a system of anarchy and no useful purpose would be solved in trying to do the same. In fact, some advocates advocated that the very idea of regulating the Internet was contradictory to the nature of Internet. However, as time passed, it began to dawn upon netizens that internet and cyberspace need to be regulated and a regulated cyberspace would be the catalyst for the future progress of mankind. Herein lay the seeds of origin of Cyber law.

There is no exhaustive definition of the term "Cyber law". However, simply stated that the, Cyber law is a term which refers to all the legal and regulatory aspects of Internet and the World Wide Web. Anything concerned with or related to, or emanating from, any legal aspects or issues concerning any activity of netizens and others, in Cyberspace comes within

the ambit of Cyber law. Cyber law is a constantly evolving process. As the Internet grows, numerous legal issues arise.

It is important to note here that due to the nature of cyber crime cannot be control by single country. Hence it needs to be regulated at four stages. Firstly, the laws made by sovereign state. Secondly it can be regulated by signing a multilateral treaty at global level. Thirdly an international organization also can make certain rule. Fourthly the cyber crime can be control by internet service provider and individual users.

In this research the main focus of researcher is to analyse the existing I.T. Act and its efficiency to combat with the cyber crime. In relation to India before 2000 there were no law's which specifically deals with the cyber crime. At that time the cyber crime was govern by the existing law. But later observation shows that it was found inadequate to control the increasing cyber crimes. Hence it was needed to amend the various existing law like Cr.P.C., Indian Evidence Act, Bankers books Evidence Act, RBI Act, Negotiable Instrument Act, Copyright Act, Patent Act, Trade Marks Act, Consumer Protection Act, etc. But still it was not enough to control the cyber crimes.

The object of the I.T. Act 2000 is to regulate the e-commerce and not to deal with the cyber crimes. But it contained some provisions relating to the cyber crimes. But those were very few. Then the gap was filled by judiciary to interpret the provisions of the existing law to cover the new kind of crime. No doubt to some extent judiciary had done it very well. But the traditional definitions of cyber crime are not coping up with the present technological advancement. Hence the need of amendment in to I.T. Act was found essential. The draft was made in this regard and I.T. [Amendment] Act, 2008 was enacted to deal with the cyber crimes. Which covered few provisions related to cyber crime at some extent but unable to fulfil the need of an hour.

Law has to keep pace with the development and this rule is more particularly applicable to information technology, a field that is very significant. With the advent of the technology and globalization the fundamental concept of Law are required to be changed. It is now felt that rapid growth is need of swift responses .The advancement of new technology requires suitable mechanism to resolve new form of dispute.

Security is the biggest obstacle for the growth of country. The internet is a notoriously insecure network, anything sent across it can be easily available .This is of particular concern when highly confidential information, such as corporate data and credit card numbers is transmitted across the internet. In want of such mechanism the internet will never be secure place for such transactions. The bottom–line is that the law should be made flexible so that it can easily adjust to the needs of the society and the technological development.

Day by day area of cyber crime is expanding and flooded with cyber crimes and existing laws are insufficient to cope up with it hence to provide new mechanism by way of cyber security is needed.

Hence In this research researcher would try to study various provisions dealing with the cyber crime and try to find out the solutions in form of cyber security.

STATEMENT OF PROBLEM:

The cyber crime is an emerging Trend. The technology has been proved boon as well as bane. The development in the science and technology has posed various problem and challenges; the cybercrime is among that at the top. Some of the major issues in conflict in the area of cyber are as follows:

1. Legal definition of "criminal conduct" is ambiguous and there is lack of global consensus on the same.

2. The lack of expertise on the part of police, prosecutors and the courts in this field.

3. The inadequacy of legal powers for investigation and access to computer systems, including the inapplicability of seizure powers intangibles such as computerized data and investigation of crime.

4. The transnational character of many cyber crimes ,and laws are insufficient to cope up with it.

These issues are required to be studied, discussed thoroughly so as to give solutions focusing security aspect; hence the researcher decided to study Global scenario of cyber crime and security provisions in comparison with legal responses in India.

IMPORTANCE OF THE STUDY

Crime is an act or omission prohibited by law. Computer can not commit crimes. However, the computer in hand in hand with the internet has given the birth to a new generation of crimes and that we called as cyber crime. Cyber crimes are the latest and most specialized evil having its origin in the computers. To control these new kinds of crimes traditional laws are not sufficient. As we say the cyber crimes are new trends in the crimes it also requires the new law and we have to find out the new security techniques to handle with it with the help of strong privacy and security laws. This problem is not only for India it is a global problem so all countries are taking steps to control this action. So there are need to frame the new laws or amend the old one which are able to cope up with new technology. India is also not an exception to it. Being a lawyer/research scholar we are duty bound to see the new challenges in the changing society. To find out the solutions to the new legal problems with the help of the judiciary. As we know that the information technology is a double-edge sword. Consistently presenting us with advantages and disadvantages, mainly the cyber crime. The nature of the cyber crime is a trans-boundary. So there are various issues relating to it such as issue of jurisdiction, identification of the accused etc. With the study of this we can find how we can handle with problem of cyber crime and provide security in form of legal provision which cope up with technological need and easy to understandable by layman. The main significance of this research is to find out the lacunas and give appropriate suggestion to combat with the problem.

In this view, to examine Indian legal position and its response to the cyber crimes and find out the cyber security techniques with help of cyber laws.

SIGNIFICANCE OF THE STUDY

Being a lawyer/research scholar we are duty bound to see the new challenges in the changing society. To find out the solutions to the new legal problems with the help of the judiciary. As we know that the information technology is a double-edge sword. Consistently presenting us with advantages and disadvantages, mainly the cyber crime. The nature of the cyber crime is a trans-boundary. So there are various issues relating to it such as issue of jurisdiction, identification of the accused etc. With the study of this we can find how we can handle with problem of cyber crime and provide security in form of legal provision which cope up with technological need and easy to understandable by layman. The main significance of this

research is to find out the lacunas and give appropriate suggestion to combat with the problem.

OBJECTIVE OF THE STUDY

Taking into consideration various objective researcher has started his research work with some of them are as follows.

1. To explore the knowledge about the crime relating to the technology and which are threat to cyber security.

2. To find out the combating capability of the laws relating to the cyber crimes.

3. To study the laws which exists in various countries in relation to the cyber crimes and security.

4. To find out the difference between the cybercrimes and conventional crimes with a security perspective.

5. To find out judicial response to the cybercrimes and security by Indian Judiciary.

6. To study various issues & challenges related to cybercrime and security s in India.

RESEARCH HYPOTHESIS

In the process of gathering information in respect of problem identification, the researcher accesses huge literature on the subject. Based on this study researcher would like to prove following hypotheses:-

1. Inception of legal provisions relating to cyber security and legal protection to cyber threat is need of an hour.

2. Traditional Laws are insufficient to curb cyber crime.

3. Recent legislative spur in area of cyber crime is not beneficial for combat cyber crime and insufficient to provide security.

4. Privacy laws are weaker to provide security in cyber space.

5. Need to inception of data protection laws.

METHODOLOGY TO BE ADOPTED:

While studying there should be certain methodology which must be follow. Every research, legal or non legal, becomes fruitful only when it is carried out in following particular research methodology. In studying this topic researcher is going to adopt doctrinal or non-empirical method of research. Researcher will also use primary data from official gazettes, treaties and conventions and codified laws.

Researcher collects secondary data from various authentic books, articles, recommendations, commentaries etc. Researcher has gone through the various books on related topic for eg. Cyber crimes Law & policy perspective, cyber Law &Crimes, Cyber Law and Its Applications, Methodology and Techniques of Social Research and will use these books for further detail study. For collection of data the researcher shall visit like N.B.Thakur Law College Library, M.V.P's Law College Library, Library of District Court, Nasik, Jayakar library, Pune, ILS Law College library ,Pune. D.E.S Law college library, Pune.

Researcher going to visits the Library of Indian Law Institute of Delhi for the purpose of collecting data and will be adhered to make the research more authentic and meaningful. The data collection will be from these sources along with various journals, articles from Law Journals like Jstore, Manupatra, Economic and political weekly etc.

Researcher also collected data from both on-line and off-line articles and through internet, magazines, news papers, etc., and various such modern and technological mechanisms available or made available from time to time whenever necessary as and when required.

In every research, research methodology is important because it provides the course of action to achieve the goal of completion of research and it is also useful in collecting data in a proper way and keeping work on the proper track.

AREA OF RESEARCH:-

The researcher tries to focus on the study cyber crime which has security concern. To solve the problem of security researcher need to study the legislation of India that is Information Technology Act 2000(Amended in 2008) and the other statute which cover the laws of security like privacy law under the Indian constitution, and these provision will compare with the global scenario of cyber security laws to provide strong piece of legislation which can curb the cyber crime and provide cyber security.

RESEARCH DESIGN:-

Researcher is planning to collect required data as early as possible. After collection of data it will analyse and interpret to test the hypothesis. The write up of thesis will be carried out after analyse data.

LIMITATION:

The researcher will focus on cyber crimes which are covered by the I.T. Act. The researcher focuses only on Sections which come under the purview of cyber crime and cyber security. And also refer the cyber crime cases relating to cyber security. Researcher is going to discuss statue of the various countries which are technologically developed and will also refer some international treaties and conventions, wherever needed.

REVIEW OF LITERATURE :

The text material related with the research work up to date sufficient to find out the exact problem that how to tackle with the reality that legal mechanisms at National and International level. This study of the researcher is the contribution towards the problem of the security relating to cyber crime in Indian scenario compare with international statute. Researcher also takes help of the statute relating to information technology act of various countries which has strong security policies to curb the cyber crime. Researcher is going to referred various literature regarding cyber crime and security which cover the legislative provisions of this area.

Researcher referred literature like Cyber laws and computer crime, Information Technology Law in which author provide depth examination and update on computer related crime including the national and international perspective with the help of data protection laws and security provisions. In this study the efforts are made towards the findings of the solution of this problem which is need of an hour.

PROPOSED WORK PLAN -

The researcher with her sincere efforts tries to complete the research work in

The following proposed time –

The collection of the data	6 Months
The critical analysis of the National and International Policies on the Cyber crime & security	1 Year
The critical analysis of the decisions of the courts under Information Technology Act	1 Year
The academic formalities with writing of the thesis with guidance of the research guide	1 Year

With tentative schedule Researcher trying to complete research proposal within Three years.

CONCEPTS AND VARIABLES:

Computer: computer is any "electronic magnetic, optical or other high speed data processing device or system which performs logical ,arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulse , and includes all input, output , processing, storage, computer software or communication facilities which are connected or related to the computer system or computer network.

Electronic : According to American law the term "electronic" means relating to technology having electric, digital, magnetic,wireless,optical,electromagnetic or similar capabilities.

Data processing device system: Data as a representation of information knowledge , facts, concepts or instructions which are being prepared or have been prepared in formalised manner , and is intended to be processed, is being processed or has been processed in a computer system or computer network , and may be in any form or stored internally in the memory of computer.

Computer resources: A computer resources as a computer, computer system, computer network, data, computer database or software.

Access: Access gaining entry into , instructing or communicating with the logical,airthmatical or memory function resources of a computer, computer system or computer network.

Information: Information includes data, text, images, sound voice, codes, computer programmes software and database or micro film or computer generated micro fiche.

Network security: Consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of acomputer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access.

Cybercrime: Is criminal activity done using computers and the Internet. This includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts. Cybercrime also includes non-monetary offenses, such as creating and distributing viruses on other computers or posting confidential business information on the Internet.

Cyberspace: It refers to the global network of interdependent information technology infrastructures, telecommunications networks and computer processing systems in which online communication takes place.

TENTATIVE SCHEME OF CHAPTERISATION:-

Chapter I

Introduction

- **Historical perspective**

Chapter II

- **Conceptual analysis of cyber crime and security**

Chapter III

Cyber crime and security – international panorama

Chapter IV

Legislative provisions & judicial response in India

Chapter V

Legislative safeguards-a comparative study

Chapter VI

Conclusion and Suggestions

- **Bibliography**
- **Web sites referred**
- **Article referred**
- **List of case Laws**

- CHAPTER - I - INTRODUCTION

  The chapterisation of the research work started with the first topic that is Introduction. This Introduction again consists with the historical perspective of cyber crime emergence and the beginning of security laws relating to information technology.

- Chapter - II – CONCEPTUAL ANALYSIS OF CYBER CRIME AND SECURITY

The second topic deal with the core concept of cyber crime and cyber security , and analysis of meaning and definition relating to cyber crime and security under the Indian statute as well as international statute.

- Chapter - III – CYBER CRIME AND SECURITY –INTERNATIONAL PANORAMA

  While studying the third chapter topics are based on the international legal instrument which are cover the scope of cyber security provision relating to cyber crime.

- Chapter - IV – LEGISLATIVE PROVISION & JUDICIAL RESPONSE IN INDIA

  In the fourth topic the researcher going to discuss the various Indian laws like information technology act 2000 (amended in 2008),constitutional law of India 1950,indian penal code 1860, Indian evidence act 1872 how this laws comes under the purview of cyber crime what are the security policies are there and judicial responses

- Chapter - V – LEGISLATIVE SAFEGUARD –A COMPARATIVE STUDY

  In the fifth topic the researcher try to frame out the legislative safe guard with the help of comparative study for the strong legislative enactment which cover all the issue of cyber crime and legislative aspect in safeguarding information and provide security laws

- Chapter - VI - CONCLUSIONS AND SUGGESTION

  In the last topic researcher will trying to conclude study with the sufficient provisions in the cyber law enactments which are helpful to provide security legislation which can curb cyber crime.

REFERENCES:

1. J.C Smith, Smith & Hogan Criminal Law Butterworth's Lexis Nexis, ISBN 0 406 94801 1] Edi. 10th.
2. Dr. Gupta and Agrawal, Cyber Laws Premier Publishing Company, 40c/34, Elgin Road, Civil Lines Allahabad- 211 001, first edition 2008.
3. Dr.R.K. Chaubey, An Introduction to Cyber Crime & Cyber law, Kamal Law House, 8/2/ksray Road, Kolkata 700 001, Edi 2008.

4. Rajan Nagia, Cyber Laws and Computer Crimes, Cyber tech Publications 4264/3, Ansari Road, Daryaganj, New Delhi-110002, First edition 2009.
5. Rohas Nagpal, Cyber Crime and Corporate Liability, Walters Kluwer pvt.ltd. New Delhi, ISBN-13; 978-81-8473-145-3, first edition, 2000.
6. Dr.Mrs.K.Sita Manikyam, CYBER CRIMES: Law & Policy Perspectives, Published by Ramesh sethi Hind law publications, 28-B, Budhwar Peth, Pune-2, 1st edition.
7. Vakul Sharma, Information Technology Law and Practice, published by Universal law publishing Co. Pvt. Ltd.C-FF-1A, Dilkhush Industrial Estate, G.T. Karnal Road, Delhi- 110 033, ISBN :978-81-7534-619-2.] 2nd Edition.
8. Parag Dewan & Shammi kapoor, Cyber and E-Commerce Laws with I.T. Act 2000 and Rules there under, published by Bharat Publishing house, New Delhi 2nd edition.
9. Lan J. Lloyd, Information Technology Law, published in the united states by oxford University Press, New York.ISBN-978-0-19-299977-5, 5TH Edition.
10. T.M. Samuel, Marial Samuel, Computer crime Information Technology Misuse, published by commonwealth publishers 44831/24, prahlad Street Ansari Road, Darya Ganj, New Delhi-110 002, ISBN-81-311-0115-0, 1st edition.
11. SV Joga Rao, Law of Cyber Crimes and I.T. Law, wadhawa and Co. Nagpur Administrative office DD-13,kalkji Extn., Opp. Neharu Place, New Delhi- 110 019 India, First edition 2004.
12. Vakul Sharma, Information Technology Law &practice, Universal Law publishing co. New Delhi India, Third edition, 2011.
13. Nirkshetri,The global cyber crime industry, Springer publication verlag berlin,heideleberg,2010
14. Barkha &U.Rama Mohan, Cyber Law &Crimes IT Act 2000&Computer crime Analysis ,Asia Law House ,Hyderabad 3rd Edition 2011.
15. Prof.shilpa.s.dongare, Cyber Law and ITS applications, current publications, Mumbai, edition 2010.

Dr. Trimbak .Bande. M
Research Supervisor

Mrs. Nivedita.B.Jadhav
Research Student